UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	S1 23 Cr. 251 (AKH)
CHARLIE JAVICE and OLIVIER AMAR,	:	
Defendants.	:	

THE GOVERNMENT'S OPPOSITION TO THE DEFENDANTS' MOTION TO SUPPRESS THE FRANK GOOGLE DRIVE MATERIALS

DANIELLE R. SASSOON
United States Attorney

Rushmi Bhaskaran
Nicholas W. Chiuchiolo
Micah F. Fergenson
Georgia V. Kostopoulos
Assistant United States Attorneys

- *Of Counsel*

TABLE OF CONTENTS

PRELIMINARY STATEMENT

The defendants' motion to suppress evidence from two Google Drive accounts—which consist of business records belonging to the defendants' former employer, J.P. Morgan Chase ("JPMC")—is utterly without merit. Dkt. 226 ("Br.").[1] Neither the factual record, nor precedent, support the existence of any Fourth Amendment violation, let alone any basis for the extraordinary remedy of suppression. Nor can the defendants seriously claim any prejudice. Of the records challenged by the defendants' motion, the Government presently intends to offer only six in its case-in-chief, all of which were produced to both defendants no later than December 2024. The defendants' motion should be denied in its entirety.

First, the Court should deny the motion for lack of standing. The defendants do not even assert—much less establish, as it is their burden to do—that they had a reasonable expectation of privacy in business records stored in work accounts owned by their former employer. Nor could they. The Google Drive accounts at issue were associated with the defendants' "@withfrank" work email addresses (the "Frank Drive Accounts") and, by the defendants' own admissions, were used to store business records. *See* Br. 4 ("Frank used Google Drive, which is a cloud-based document storage system, as a central repository for documents related to its business."); Jan. 23, 2025 Tr. at 50:17-19 (counsel for Javice describing the Frank Drive Accounts as being used by the defendants for "their work at Frank" such as "edit[ing] a spreadsheet"). By virtue of its acquisition of Frank, JPMC has owned these business records since 2021. And at the time of the seizure, the defendants were not even employees of JPMC and had no rights whatsoever to access, possess, or exclude others from the Frank Drive Accounts owned by JPMC. Simply put, the defendants lacked a

[1] Javice joined the brief filed by Amar. Dkt. 229.

reasonable expectation of privacy in these documents and spreadsheets belonging to JPMC, and the defendants do not attempt to argue otherwise. The Court should deny the motion on this ground alone.

Second, even assuming, *arguendo*, that the defendants had a personal privacy interest in JPMC's business records—and they plainly do not—the defendants' motion should be denied because the Government's review of the Frank Drive Accounts was reasonable and complied with the Fourth Amendment in all respects. Numerous courts in this Circuit have held that reviews of electronic evidence are not unreasonable because they continue over months and even years. The review here of nearly 100,000 files over approximately one year, conducted pursuant to a judicially authorized search warrant, did not violate the Fourth Amendment.

Rather than engaging with the governing law and accurate facts, the defendants devote the vast majority of their motion to accusing the Government of acting in bad faith based on nothing more than unfounded speculation. Yet the simple reality, evident from the record (which the defendants do their best to render confusing), is that the Government's review of the Frank Drive Accounts was ongoing after April 2024. In an effort to conjure the specter of a constitutional issue, the gravamen of the defendants' motion is that this fact is somehow "not credible" (Br. 2) and even a "misrepresentation" (Br. 3). The defendants' accusations are groundless. The fact that the Government's review extended past April 2024 into January 2025 is simply what occurred. The defendants' baseless speculation is not a basis for finding a Fourth Amendment violation, and certainly does not provide a reason to suppress evidence. *See, e.g.*, *United States v. Aguilar*, 20 Cr. 390 (ENV), Dkt. 160 at 9 (E.D.N.Y. July 7, 2023) (defendant's "speculation regarding the precise timeline and methodology of the government's review . . . make[s] no difference, given . . . the review fit within acceptable bounds and the seizure was proper").

The defendants' motion should be summarily denied as there is no merit to the defendants' arguments in favor of suppression. Nor is some further alternative remedy related to the Google Drive materials warranted. As discussed at the January 23, 2025 conference, the Government acknowledges that, due to an oversight by the Government, the materials in its final joint-production of Google Drive records in January 2025 should have been globally produced earlier. The Court has already granted the defendants a one-week adjournment to facilitate their review of what is new to each defendant within those records, even though the Government is not seeking to use those documents in its case-in-chief. The defendants are aware of the six Google Drive files the Government presently intends to offer in its case-in-chief, which were globally produced no later than December 2024, months before trial. There is absolutely no basis for a third adjournment of this trial.

BACKGROUND

On or about October 6, 2023, the Honorable Stewart D. Aaron, United States Magistrate Judge for the Southern District of New York, signed a search warrant (the "Warrant") authorizing the search and seizure of records, including Google Drive files, maintained by Google and associated with the email addresses "charlie@withfrank.org" (the "charlie@withfrank Drive Account") and "olivier@withfrank.org" (the "olivier@withfrank Drive Account"; together with the charlie@withfrank Drive Account, the "Frank Drive Accounts"). *See* Dkt. 226-1 at 29-34 ("Warrant"). The Frank Drive Accounts were associated with the defendants' respective work email addresses and used to store Frank's business records. The Warrant was supported by a sworn affidavit (the "Affidavit"). *See* Dkt. 226-1 ("Aff.") at 1-28. As noted, the Warrant authorized the seizure of, among other things, Google Drive files. Warrant at 6; Aff. ¶ 4(c)(ii). Google Drive is an online storage platform that can be used to store "email, attachments, videos, photographs,

documents, and other content . . . online." Aff. ¶ 4(c)(ii). Accountholders can share files with others, in addition to viewing, commenting, and editing those files. Aff. ¶ 4(c)(ii). Google Drive supports different file types, including word documents and spreadsheets. Aff. ¶¶ 4(c)(ii)-(iii).

The Government served the Warrant on Google on October 6, 2023—*i.e.*, the same day the Warrant was signed by Magistrate Judge Aaron. After receiving the files from Google on October 10, 2023, and after receiving a set of external hard drives from the defense, on or about October 31, 2023, the Government produced the full contents of the charlie@withfrank Drive Account to Javice, and the full contents of the olivier@withfrank Drive Account to Amar.[2] The total size of both productions was approximately 97,439 files: approximately 8,984 files to Javice, and approximately 88,452 files to Amar.[3]

The prosecution team first obtained access to the files on its own search-ready electronic database on or about January 19, 2024.[4] Between that date and the present, and on a rolling basis,

---

[2] The Government proceeded in this manner, rather than producing both Frank Drive Accounts to both defendants, pursuant to the current practice of the U.S. Attorney's Office, which was adopted in response to claims by defendants that cross-production of seized electronic accounts itself violated the Fourth Amendment. *See United States v. Reichberg*, 5 F.4th 233, 239 (2d Cir. 2021) (upholding denial of suppression where defendant claimed that the cross-production of data from his electronic devices and accounts to co-defendants "worked an independent unreasonable seizure in violation of the Fourth Amendment," while assuming for the "sake of discussion" that such discovery productions to co-defendants could constitute a Fourth Amendment violation); *United States v. Archer, et al.,* S1 16 Cr. 371 (RA) (Dkt. No. 212) (Aug. 3, 2017) (addressing defense objections to Government productions, where the Government had produced the entire contents of certain email accounts to all co-defendants).

[3] In his brief, Amar states that the Google Drive production to him was "almost 160,000 documents." Br. 7. The Government's calculation of the number of documents produced to both Amar and Javice comes from the electronic database onto which the Government loaded the materials it provided to the defendants on or about October 31, 2023.

[4] Consistent with the Government's practice, particularly for large volumes of electronic material, after producing the entirety of the Google Drive materials associated with each account to each respective defendant, the same materials were then loaded into an online platform in order to facilitate the Government's review. *See* Fed. R. Crim. P. 41(e)(2)(B) (providing that the

the Government made approximately three global productions of responsive materials to both defendants from the Google Drive materials, on or about: (1) April 29, 2024; (2) December 17, 2024; and (3) January 22, 2025.[5] In total, the Government marked and produced approximately 28,000 documents as responsive. The Government's responsiveness review pursuant to the Warrant concluded on or about January 21, 2025—approximately one year after the Government obtained access on its review platform to approximately 97,000 files obtained pursuant to the Warrant. The Government's review was ongoing in this time period, and at no time was the Government's review closed and then reopened.

On or about January 21, 2025, and in the course of concluding the Government's review, the Government became aware that approximately 13,000 files that had been previously marked as responsive over the course of the Government's then-ongoing responsiveness review had not been globally produced to both defendants. Of those files, approximately 3,709 files were from the charlie@withfrank Drive Account (and had been previously produced in full to Javice); and approximately 9,559 files were from the olivier@withfrank Drive Account (and had been previously produced in full to Amar).[6] The Government promptly alerted the defendants to the

---

Government may seize "electronic storage media or . . . electronically stored information" for "a later review of the media or information consistent with the warrant."). Rule 41 also explicitly authorizes the Government to retain a copy of electronic media seized pursuant to a warrant. *See* Fed. R. Crim. P. 41(f)(1)(B) ("The officer may retain a copy of the electronically stored information that was seized or copied.").

[5] At the defendants' request, on or about January 16, 2025, the Government re-produced its December 17, 2024 responsiveness production in an alternative format in order to facilitate the defense's review.

[6] Of the total volume of approximately 13,000 files, and according to metrics provided by the Government's online review platform, approximately 60 percent are duplicate files. In total, the Government identified approximately 3,104 unique files that had not been previously produced to Javice, and approximately 2,150 unique files that had not been previously produced to Amar.

forthcoming production, and expedited the production to both defendants the following day, on January 22, 2025. The Government made this production despite the fact that it did not intend to use any of the newly-produced documents in its case-in-chief at trial. The next day, on January 23, 2025, the parties appeared before the Court for a conference to address pending motions. At the conference, the defendants requested an adjournment of the forthcoming trial in light of the recent production. The Court granted the defendants' request and ordered a one-week adjournment of trial, which is now scheduled to begin on February 18, 2025.

Since that time, the Government has engaged in a good-faith effort to facilitate the defendants' review of the Google Drive materials, including engaging in a series of lengthy telephone calls and written correspondence about the Google Drive materials. As part of those efforts, the Government answered detailed questions about the format of the Google Drive materials, and attempted to provide metrics to guide the defendants' review of the Google Drive materials. Additionally, both of its own accord and at the Court's direction, of the approximately two hundred Google Drive-related exhibits identified on the Government's exhibit list back in December 2024, the Government narrowed its exhibit list and identified just six exhibits it currently intends to offer from the Google Drive materials. These six exhibits had been marked as responsive no later than May 2024. Three of the six exhibits had been produced to both defendants on April 29, 2024, and the remaining half were produced to both defendants on December 17, 2024—*i.e.*, eight weeks before trial. None of the six exhibits were part of the Government's final responsiveness production made in January 2025.

LEGAL STANDARD

The Fourth Amendment prohibits "unreasonable searches and seizures." U.S. Const., amend. IV. This includes a requirement that, when evidence is seized pursuant to a warrant, that

warrant must both be facially reasonable and be executed in a reasonable manner. *See United States v. Ganias*, 824 F.3d 199, 209–10 (2d Cir. 2016) (*en banc*). When a search or seizure is unreasonable, courts may impose an appropriate remedy, including, as a "last resort," suppression of evidence collected pursuant to the unreasonable search or seizure. *Davis v. United States*, 564 U.S. 229, 237 (2011) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)).

A defendant seeking suppression "has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." *See Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978); *United States v. Pena*, 961 F.2d 333, 336 (2d Cir. 1992). "It is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search." *United States v. Ruggiero*, 824 F. Supp. 379-391 (S.D.N.Y. 1993) (citations omitted), *aff'd sub nom*. *United States v. Aulicino*, 44 F.3d 1102 (2d Cir. 1995). When an affidavit or other evidence is submitted, a defendant asking a court to suppress evidence must still meet his or her burden of showing a legitimate expectation of privacy in the area that was searched. *Id.*; *see also Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980).

Even where a Fourth Amendment violation is found in the execution of a warrant, it does not automatically follow that suppression is warranted. "Courts have [ ] indicated that the drastic remedy of the suppression of all evidence seized is not justified unless those executing the warrant acted in flagrant disregard of the warrant's terms." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) (internal quotation marks omitted). "Government agents 'flagrantly disregard' the terms of a warrant . . . only when (1) they effect a widespread seizure of items that were not within the

scope of the warrant, and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal citations omitted).

ARGUMENT

The motion to suppress is meritless. Under well-settled law, the defendants did not have any reasonable expectation in these business accounts and records belonging to their former employer, and the defendants do not attempt to argue otherwise. Their Fourth Amendment rights were not violated. Nor was there any Fourth Amendment violation whatsoever. The Government obtained a lawful warrant and conducted a reasonable responsiveness review of electronic records. In addition to acting in accordance with the Fourth Amendment, the Government has acted in good faith. The defendants' attempts to impugn the good faith of the Government are baseless and do not withstand even the most basic scrutiny. The Court should thus summarily deny the motion on at least three independent grounds: (1) the defendants lack standing, (2) the Government's review was reasonable, and (3) the Government acted in good faith.

I. The Defendants Lack Standing To Challenge a Seizure of JPMC's Property

The defendants' motion fails at the very outset because the defendants lack standing under the Fourth Amendment. The defendants do not even assert, much less establish, that, in October 2023, they had a reasonable expectation of privacy in these business accounts belonging to their former employer, JPMC, and for which they had no right to access, no right to possess, and no right to exclude others—nor any other personal or proprietary interest of any sort. Accordingly, the defendants lack standing to challenge a search and seizure of JPMC's property, and the Court can deny the motion on that basis alone.

A. Relevant Facts

On August 8, 2021, Frank and JPMC executed the Merger Agreement.[7] As set forth in the agreement, "all of the property, rights, privileges, immunities, powers and franchises of [Frank] . . . shall vest in" JPMC. Merger Agreement ¶ 2.5. Among the property that was conveyed to JPMC in the merger were Frank's electronic business systems and applications. As reflected in the Merger Agreement, "[a]ll Systems are either owned by, licensed or leased to" Frank, *id.* ¶ 3.16(k); and the Agreement defined "Systems" as "the Software, hardware, firmware, networks, platforms, servers, interfaces, applications, websites and related information technology systems used by any member of [Frank] in connection with the business of [Frank]."[8] *Id.* at 17.

In September 2021, the transaction closed and JPMC acquired Frank and all of its business servers, systems, and applications—including any Google Drive accounts associated with "@withfrank" email addresses and used for Frank's business, such as the Frank Drive Accounts at issue here.

At or about the time that the merger became effective, the defendants became employees of JPMC. Approximately a year later, in late 2022, the defendants were terminated by JPMC.

In October 2023—approximately one year after the defendants' employment with JPMC had ceased, and two years after they had sold their Frank business systems to JPMC—the Government obtained and served the Warrant for the Frank Drive Accounts owned by JPMC.

---

[7] Technically, the transaction was structured such that Frank merged with a JPMC subsidiary set up for purposes of the acquisition. For ease of exposition, this summary discusses the transaction in simplified terms.

[8] "Software" was in turn defined as "(a) all computer generated programs, including source code and object code versions, and (b) all databases, whether machine readable or otherwise." Merger Agreement at 16.

B. Applicable Law

"It has been clear for a generation that 'Fourth Amendment rights are personal rights . . . [that] may not be vicariously asserted.'" *United States v. Haqq*, 278 F.3d 44, 47 (2d Cir. 2002) (quoting *Rakas*, 439 U.S. at 133-34). Accordingly, a defendant's Fourth Amendment rights are violated "only when the challenged conduct invaded his legitimate expectation of privacy rather than that of a third party." *United States v. Payner*, 447 U.S. 727, 731 (1980); *see also United States v. Villegas*, 899 F.2d 1324, 1333 (2d Cir. 1990) ("A defendant has no right to have evidence suppressed on Fourth Amendment grounds unless the breached privacy expectation was his own rather than that of a third party.").

Ultimately, the Fourth Amendment's standing inquiry is "whether defendant has established a legitimate expectation of privacy in the area searched." *United States v. Chuang*, 897 F.2d 646, 649 (2d Cir. 1990) (*citing United States v. Rahme*, 813 F.2d 31, 34 (2d Cir. 1987)). This threshold question involves two separate inquiries: (1) whether a defendant has demonstrated a subjective expectation of privacy in the places and items that were searched; and (2) whether that expectation was one that society accepts as reasonable. *Id.*

"One who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of th[e] right to exclude." *Rakas*, 439 U.S. at 143 n.12. When a person conveys or abandons property, however, "he forfeits any reasonable expectation of privacy that he might have had in the property." *United States v. Lee*, 916 F.2d 814, 818 (2d Cir. 1990). In fact, "[n]either possession nor ownership of property establishes a legitimate expectation of privacy unless the party vigilantly protects the right to exclude others." *United States v. Torres*, 949 F.2d 606, 608 (2d Cir. 1991); *see also id.* at 607 ("It is well settled that an otherwise legitimate

privacy interest may be lost by disclaiming or abandoning property, especially when actions or statements disavow any expectation of privacy.").

When courts assess searches related to an employee, "defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched." *United States v. Kazarian*, No. 10 Cr. 895 (PGG), 2012 WL 1810214, at *18 (S.D.N.Y. May 18, 2012) (citing *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987)). Even where there is a subjective expectation of privacy in this setting, it gives rise to standing only where that expectation is one society considers reasonable. *See Chuang,* 897 F.2d at 650 (any subjective belief bank officer had in privacy of documents maintained at bank's premises objectively unreasonable given extensive regulation of banks). Where an employee lacks any personal or proprietary interest in a business's electronically stored information, he has no reasonable expectation of privacy in the business's materials. *See United States v. Triumph Cap. Grp., Inc.*, 211 F.R.D. 31, 53–54 (D. Conn. 2002) ("There is no evidence that [an employee] had any personal or proprietary interest in the laptop computer."); *accord Chuang*, 897 F.2d at 649 ("To show a legitimate expectation of privacy, an employee must have a 'possessory or proprietary interest in the area searched.'").

"When considering a claimed violation of Fourth Amendment rights, the burden is on the defendant to establish that his own rights under the Fourth Amendment were violated." *United States* v. *Paulino*, 850 F.2d 93, 96 (2d Cir. 1988).

C. Discussion

The defendants lack standing under the Fourth Amendment to challenge the Warrant seizing the Frank Drive Accounts, which held business records belonging to the defendants' former employer, JPMC. The Court can deny the motion to suppress on that basis alone.

To start, the defendants clearly had no property interest in the Frank Drive Accounts. As reflected in the Merger Agreement signed by Javice herself, Frank owned the Frank Drive Accounts and then conveyed all of its rights and ownership in those accounts to JPMC.[9] Moreover, the defendants lacked any possessory interest in the Frank Drive Accounts. At the time the warrant was executed, the defendants were not even employees of, or otherwise associated with, JPMC, and they had no right to access, possess, or exclude others from the Frank Drive Accounts, which were owned by their former employer, JPMC. *See Kazarian*, 2012 WL 1810214, at *18 ("defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched").

The defendants do not even *assert* in their brief, much less meet their burden of establishing, that they held some kind of personal privacy interest in the Frank Drive Accounts.[10] If anything, the defendants' brief and their representations to the Court make clear that the opposite

[9] Additionally, once the Frank Drive Accounts became the business records of JPMC, and the defendants became employees of JPMC, even assuming there were some kind of personal privacy interests in the Frank Drive Accounts—and they were none, as explained herein—any such interest would have been extinguished as JPMC is a heavily regulated financial institution. *See Chuang*, 897 F.2d 646 at 650 (any subjective belief bank officer had in privacy of documents maintained at bank's premises objectively unreasonable given extensive regulation of banks).

[10] Neither defendant submitted a sworn affidavit, and that failure alone is sufficient to deny the motion. *See, e.g.*, *United States v. Ruggiero*, 824 F. Supp. 379-391 (S.D.N.Y. 1993) ("It is well established that in order to challenge a search, a defendant must submit an affidavit from someone with personal knowledge demonstrating sufficient facts to show that he had a legally cognizable privacy interest in the searched premises at the time of the search."); *United States v. Tranquillo*, 606 F. Supp. 2d 370, 378 (S.D.N.Y. 2009) ("As a preliminary matter, [defendant] has not put forth the foregoing facts—or, indeed, *any* facts relevant and probative of his privacy interest in the [seized computers]—in a sworn affidavit."); *United States v. Sorcher*, No. 05 CR 0799 NG RLM, 2007 WL 1160099, at *8 (S.D.N.Y. Apr. 18, 2007) ("Indeed, the record contains no affidavits from defendants asserting their possessory or proprietary interest in the documents.").

is true: the defendants concede that the Frank Drive Accounts were used to store *business* records—all of which are now the business records of JPMC. *See* Br. at 4 ("Frank used Google Drive, which is a cloud-based document storage system, as a central repository for documents related to its business."); *see also* Jan. 23, 2025 Tr. at 50 (counsel for Javice describing the Frank Drive Accounts as being used by the defendants for "their work at Frank" such as "edit[ing] a spreadsheet").

Underscoring the fact that the defendants have no reasonable expectation of privacy in these materials is the fact that JPMC currently has access to them. As described in the Warrant's affidavit, JPMC did not have access to all of the Google services used by Frank at the time of the Warrant. *See* Affidavit at 14 n.6. The Government understands that JPMC can now access the Frank Drive Accounts. In other words, the Government could obtain records from the Frank Drive Accounts (tied to the defendants' "@withfrank.org" email accounts), in the same way that the Government obtained the entirety of the defendants' "@withfrank.org" email mailboxes—pursuant to a subpoena. The defendants have never claimed, or even suggested, that the Government's obtaining their work email accounts without a warrant violated their privacy rights. Nor could they. The defendants have no reasonable expectation of privacy in business records that belong to JPMC by virtue of the Merger Agreement—whether those records are the Frank email accounts produced by JPMC in response to a subpoena or, as here, the Frank Drive Accounts produced by Google in response to the Warrant.

In short, because the defendants lacked any personal, possessory, or proprietary interest in the Frank Drive Accounts, they had no reasonable expectation of privacy in the Frank Drive Accounts and lack standing under the Fourth Amendment to challenge the Warrant's seizure of business records that belong to JPMC, their former employer and a victim of their fraud. *See, e.g.*,

Chuang, 897 F.2d at 649 ("To show a legitimate expectation of privacy, an employee must have a possessory or proprietary interest in the area searched."); *Triumph Cap. Grp., Inc.*, 211 F.R.D. 31, 53–54 (denying motion to suppress for lack of standing because "[t]here is no evidence that [an employee] had any personal or proprietary interest in the laptop computer"). Accordingly, the motion to suppress should be denied.

II. The Government's Review Was Reasonable In Any Event

Even assuming the defendants had privacy interests in JPMC's business records, the Government fully complied with the Fourth Amendment, including by conducting a reasonable responsiveness review of the Frank Drive Accounts.

A. Applicable Law

While "'the reasonableness of government conduct in executing a valid warrant . . . can present Fourth Amendment issues,'" it is nevertheless the case that "searches performed pursuant to a warrant . . . 'will rarely require any deep inquiry into reasonableness.'" *United States v. Sosa*, 379 F. Supp. 3d 217, 222 (S.D.N.Y. 2019) (quoting *United States v. Ganias*, 824 F.3d 199, 209 (2d Cir. 2016) (en banc)). "[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant[.]" *Dalia v. United States*, 441 U.S. 238, 257 (1979). For searches authorizing the seizure of electronically stored information, "the Fourth Amendment does not require a search warrant to specify computer search methodology." *United States v. Bowen*, 689 F. Supp. 2d 675, 681 (S.D.N.Y. 2010). Accordingly, courts "reviewing challenges to searches of electronically stored information have declined to require any particular protocols such as the use of specific search terms or methodologies." *United States v. Lebovits*, 11 Cr. 134 (SG), 2012 WL 10181099, at *22 (E.D.N.Y.

Nov. 30, 2012), report and recommendation adopted *sub nom*. *United States v. Gutwein*, 11 CR 134 (SG), 2014 WL 201500 (E.D.N.Y. Jan. 16, 2014).

Search warrants also need not prescribe a specific protocol *ex ante*, and courts do not require any specific protocol in reviewing the reasonableness of a search *ex post*. *See, e.g.*, *United States v. Lumiere*, 16 Cr. 483 (JSR), 2016 WL 7188149, at *4 (finding search reasonable where agent did not follow formal document review protocol, did not mark documents "responsive" and "not responsive," and did not "otherwise memorialize his findings"). Instead, where a warrant authorizes "various techniques to locate information responsive to the warrant," courts recognize that searches conducted in a flexible manner are reasonable and "appropriate." *United States v. Mendlowitz*, 17 Cr. 248 (VSB), 2019 WL 1017533, at *12 (S.D.N.Y. Mar. 2, 2019) (internal quotations and citations omitted).

The reasonableness standard also affords significant flexibility as to the duration of a search. The Advisory Committee Notes to Rule 41(e)(2) states in part that "the practical reality is that there is no basis for a 'one size fits all' presumptive period." Fed. R. Crim. P. 41(e)(2) (advisory committee's note to 2009 amendments). There is thus "no established upper limit as to when the government must review seized electronic data to determine whether the evidence seized falls within the scope of a warrant." *Sosa*, 379 F. Supp. 3d at 222 (internal quotation marks omitted). Accordingly, lengthy periods of review of seized electronic data have been upheld without a requirement of any detailed accounting, or even any explanation at all, from the Government for the review's length. *See, e.g.*, *United States v. Olivo*, No. 22 Cr. 582 (VEC), 2023 WL 8432864, at *3 (S.D.N.Y. Dec. 5, 2023) (denying motion to suppress where Government did not begin reviewing seized cellphone for several months, concluding that delays were not "so extreme as to violate" the defendant's rights); *Aguilar*, 20 Cr. 390 (ENV), Dkt. 160 at 5-10

(denying defendant's motion to suppress responsive materials collected following two-and-a-half-year long review); *Sosa*, 379 F. Supp. 3d at 222 (15-month and 10-month review periods reasonable even though "the reasons for the delays" were "not made explicit in the record"); *United States v. Estime*, 19 Cr. 711 (NSR), 2020 WL 6075554, at *14-15 (S.D.N.Y. Oct. 14, 2020) (delay of ten months reasonable); *Mendlowitz*, 2019 WL 1017533, at *12 (upholding 18-month review period as reasonable); *United States v. Nejad*, 436 F. Supp. 3d 707, 736 (S.D.N.Y. 2020) (denying motion to suppress responsive materials identified as part of review that ranged between one and three years in total, "[g]iven the volume of documents, the various obstacles to review, and the resource constraints . . .").

B. Discussion

The basic facts of the Government's execution of the Warrant and review of the returns suffice to deny the defendants' motion. The Government served the Warrant on Google the same day it was signed. After receiving the files, the Government promptly made individual full productions of the charlie@withfrank.org Drive Account to Javice, and the olivier@withfrank.org Drive Account to Amar. Given the volume and type of files provided by Google, the Government loaded the files to its review platform, and obtained access to the materials from the Frank Drive Accounts on its review platform in January 2024. The Government then reviewed those materials, which spanned nearly a hundred thousand files, over a span of approximately twelve months, making three responsive productions to the defense. The materials that were seized and deemed responsive were within the heartland of the warrant, and include business records and documents created, edited, and exchanged by the defendants. Neither the timing nor the sequence of the review, or the duration of time that the review took, was unreasonable for a review of nearly 100,000 electronic files. Indeed, "numerous cases have held that 'a delay of several months or

even years between the seizure of electronic evidence and the completion of the government's review of it is reasonable.'" *Aguilar*, 20 Cr. 390 (ENV), Dkt. 160 at 6 (quoting *Sosa*, 379 F. Supp. 3d at 222)(collecting cases)); *see also United States v. Almaleh*, 17 Cr. 25 (ER), 2022 WL 602069, at *20 (S.D.N.Y. Feb. 28, 2022) (denying motion to suppress where evidence where defendant was provided with rolling productions over a fifteen-month period); *Mendlowitz*, 2019 WL 1017533, at *12 (S.D.N.Y. Mar. 2, 2019) (finding a review process of 18 months reasonable).

In the face of these authorities—and putting aside the defendants' repeated, baseless allegations of governmental concealment, misrepresentation, and misconduct—the defendants' argument regarding the reasonableness of the review appears limited to two paragraphs in their brief, which in turn relies on a single out-of-circuit case. *See* Br. 9-10 (citing *United States v. Cawthorn*, 682 F. Supp. 3d 449, 459 (D. Md. 2023)). That sole authority, however, is easily distinguishable and not persuasive. *Cawthorn* concerned the review of a search warrant return for a single Instagram account in a gang case where the government's review spanned approximately two-and-a-half years.[11] *See Cawthorn*, 682 F. Supp. 3d at 459 & n.7. The review in this case, by contrast, was completed in a one-year period (less than half the time in *Cawthorn*) and concerned two Google Drive accounts used to store nearly 100,000 business records in the context of a complex white-collar fraud investigation. More to the point, a single out-of-circuit decision simply does not overcome the contrary and consistent authority from numerous courts in this Circuit, which "have routinely found reviews even more directly analogous to this one to be reasonable." *Aguilar*, 20 Cr. 390 (ENV), Dkt. 160 at 6 (E.D.N.Y. July 7, 2023). In fact, even the few in-district

[11] Further, even the court in *Cawthorn* did not endorse the extreme remedy the defendants seek—wholesale suppression of the entire contents of the warrant—but only suppressed the materials the Government had identified during subsequent, supplemental reviews conducted two years after the execution of the warrant. *See Cawthorn*, 682 F. Supp. 3d at 459.

cases relied on by the defendants do not even support their position regarding the reasonableness of this review's length. *See, e.g.*, *Nejad*, 436 F. Supp. 3d at 735 (holding that a responsiveness review that continued "roughly three years after issuance of the first search warrant in April 2014 and only one year after issuance of the last warrant in 2016" was "reasonable under the circumstances" given the size and complexity of the returns).[12]

The other cases relied on by defendants involved vastly different circumstances than those presented here. This review—and the underlying warrant authorizing it—could not be more different from *United States v. Wey*, 256 F. Supp. 3d 355, 395 (S.D.N.Y. 2017), which the defendants rely on throughout their motion. In *Wey*, Judge Nathan suppressed certain evidence on the grounds that the search warrants at issue were facially deficient and that the resulting searches could not be saved by the good-faith exception. *Id.* at 384-399. In the course of her decision, Judge Nathan criticized various aspects of the execution of the search warrants as they pertained to electronic evidence seized in the particular circumstances of that case. *Id*. at 399-408. Among other things, Judge Nathan expressed concern about the duration of the searches, which took place over the course of several years, and the repeated efforts of law enforcement to search data initially identified as non-responsive. *Id*. Judge Nathan did not, however, reach the question of whether

[12] The defendants' contention, repeated throughout their brief, that the Government's actions here bear any similarity to the second *Nejad* decision is similarly inapt. *United States v. Nejad*, 487 F. Supp. 3d 206, 211 (S.D.N.Y. 2020) ("*Nejad II*"). In *Nejad II*, the Court concluded that federal law enforcement agents improperly conducted a search of certain email returns obtained by a state prosecutor's office because the search exceeded the scope of the state court warrants, and had failed to disclose potentially exculpatory documents until after trial had concluded. Much like the other unfounded assertions of Government misconduct that permeate the defendants' brief, apart from gesturing towards the specter of *Nejad II*, the defendants do not meaningfully explain how this case—where the Government obtained a valid warrant, searched certain records, promptly produced those records to the defendants, and then produced responsive returns from those records in advance of trial—bears any resemblance to *Nejad II.*

these concerns rose to the level of independent Fourth Amendment violations. This case, by contrast, does not implicate the Fourth Amendment concerns set forth in *Wey*'s dicta. As noted above, the Government reviewed the Frank Drive Accounts in the immediate months following its receipt of that account and identified certain responsive materials. Moreover, absent a further warrant, the Government does not intend to introduce (or re-review) evidence from that account beyond the evidence it identified during the initial review. As such, the fact pattern in *Wey*—where these steps were not taken—render those decisions inappropriate touchstones on which to evaluate the Government's conduct in this case.

United States v. Galpin, 720 F.3d 436 (2d Cir. 2013) is similarly inapposite. In *Galpin*, the Second Circuit invalidated a search warrant itself for being impermissibly broad, and for its failure to establish probable cause to search for evidence of child pornography. *Id.* at 453 (finding there was "ample evidence that investigators sought evidence beyond the scope of the one crime that was particularized in the warrant application and for which the application supplied probable cause."). The defendants cannot credibly claim that this review—which was well-bounded by the warrant, tethered to the allegations identified therein, and spanned roughly a year from start to finish—bears any resemblance whatsoever to the reviews described in *Wey* and *Galpin*. Indeed, the defendants do not claim that the underlying warrant was invalid, a challenge that was at the heart of the suppression decisions in both *Galpin* and *Wey*.

Simply put, the Government's approximately one-year review of nearly 100,000 records obtained pursuant to a valid warrant was reasonable, as established by significant authority within this Circuit, and the defendants' arguments to the contrary are unpersuasive.

III. The Government Acted In Good Faith

Rather than engage with their lack of any privacy interests in the Frank Drive Accounts, or the ample authority that a one-year review of records like those at issue here is reasonable under the Fourth Amendment, the defendants instead repeatedly assert that this case evinces some sort of extraordinary governmental misconduct. The defendants are wrong and their assertions have no basis in fact. The Government acted in good faith in obtaining and executing the Warrant and in reviewing the materials in the Frank Drive Accounts, as well as in conferring with defense counsel regarding its January 2025 production. There is no merit to the defendants' groundless claims.

In particular, the defendants repeatedly speculate that "it is far more likely that the Government did in fact conclude its responsiveness review earlier in 2024"—specifically, on April 29, 2024. Br. 10. The defendants are incorrect. Without a shred of evidence to support their assertions, the defendants are accusing the Government of lying, first to the defendants, and then to the Court. That accusation is a significant one to make to this Court. It is also nonsensical. Take, for example, just a few basic facts already set out in the defendants' brief. The Government made its first responsiveness production on April 29, 2024. *See* Br. 5. As the prosecution team's review was still ongoing, the very next month—*i.e.*, within days of the April 29, 2024 production—the prosecution team tagged additional documents from the Frank Drive Accounts as responsive. *See* Br. 6 (noting the Government explained in written correspondence that all but one of the 82 documents it produced in December 2025 had been tagged responsive back in May 2024). This straightforward record does not in any way suggest a "closing" of the responsiveness review in April 29, 2024 and its "reopening" days later. Rather, as the Government has consistently

explained to the defendants in response to their repeated questions, and as the Government has represented truthfully to the Court, the Government's responsiveness review was ongoing.

Similarly, the defendants baselessly suggest that the Government *must* have closed and then reopened its review only in December 2024, in order to gain a tactical advantage from newly-disclosed information, such as the defendants' exhibit and witness lists. *See* Br. 11 (speculating the Government re-opened its review "after months of gleaning additional information from witness interviews, subpoena returns, motion practice, and ultimately the Defendants' witness lists and exhibit lists," which the Government purportedly used to "search for additional documents to bolster its prosecution of Defendants based on theories not formed at the time it requested the search warrant and information not presented to Magistrate Judge Aaron"); *id.* at 2 (same); *id.* at 9 (same).

This contention is equally nonsensical and belied by straightforward facts.[13] The defendants did not produce their witness or exhibit lists until January 6, 2025. The Government made only one responsiveness production thereafter, consisting of records that the Government *does not intend to use in its case*. The six files from the Frank Drive Accounts that the Government *does* presently intend to use in its case—consisting of two spreadsheets and one word document, as well as the three metadata logs that correspond to those three files—were globally produced (and, indeed, marked as exhibits) *prior* to the defendants' trial disclosures, no later than December 17, 2024. In fact, far from being the result of "search[es] for additional documents to bolster its prosecution of Defendants based on theories not formed at the time it requested the search warrant

[13] Of course, this argument can also easily be rejected because there is no requirement that when executing a search, the Government is confined only to particular "theories" or fully formed views of the evidence. A search is an investigative technique, used to investigate specified crimes.

and information not presented to Magistrate Judge Aaron," as the defendants allege, two of the three documents (excluding metadata logs) that the Government intends to offer at trial *are described in the affidavit accompanying the Warrant itself*.[14] *See* Aff. ¶ 18(d) (describing an email reflecting that Javice had invited Amar to edit a Google spreadsheet named "User_Breakdown_CJ_v2"); *id.* ¶ 18(f) (describing an email reflecting that Javice had invited Amar and Engineer-1 to edit a Google document named "Data_Request").

Accordingly, the defendants' accusations and insinuations of bad faith and misconduct are speculative and ultimately nothing more than wishful thinking of finding a constitutional claim to exploit. They are also nonsensical and contradicted by the factual record. For the same reasons that the Government's review was reasonable and consistent with the Fourth Amendment, suppression is clearly not warranted because the Government acted in good faith. *See United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000).

IV. A Hearing Is Not Required To Deny the Defendants' Motion

The defendants have not demonstrated the need for an evidentiary hearing. As the movants, the defendants bear the burden of "showing the existence of disputed issues of material fact." *United States v. Martinez*, 992 F. Supp. 2d 322, 326 (S.D.N.Y. 2014) (quoting *United States v. Washington,* 12 Cr. 146 (JPO), 2012 WL 5438909, at *8 (S.D.N.Y. Nov. 7, 2012)). The defendants come nowhere close to meeting their burden. As to standing, there appears to be no dispute that

[14] Additionally, the Government explicitly identified and described the third document—named "Records Needed" and created on August 3, 2024—that it intends to offer at trial in a December 13, 2024 call with counsel for Amar, when discussing a potential pretrial resolution. Further, Amar's brief makes clear that he has possessed all of these documents since 2023 when he received a copy of the full olivier@withfrank Drive Account. *See* Br. 7 (describing how the two documents that derive from the charlie@withfrank Drive Account are "identical copies of documents from" the olivier@withfrank Drive Account).

the Frank Drive Accounts contained business records, not personal records in which the defendants might have a reasonable expectation of privacy, and the defendants have not even filed an affidavit in connection with their motion to claim standing. There can similarly be no dispute that the defendants sold their property interests in Frank and its electronic business records to JPMC years before the Warrant. The Government nonetheless searched the Frank Drive Accounts pursuant to a judicially-authorized search warrant, and executed that search in a reasonable manner. With respect to the reasonableness of the review, all of the defendants' "speculation regarding the precise timeline and methodology of the government's review . . . make[s] no difference, given . . . the review fit within acceptable bounds and the seizure was proper." *Aguilar*, 20 Cr. 390 (ENV), Dkt. 160 at 9. A hearing is thus not warranted because the defendants have failed to demonstrate that "contested issues of fact going to the validity of the search are in question." *United States v. Pena*, 961 F.2d 333, 339 (2d Cir. 1992) (quoting *United States v. Licavoli,* 604 F.2d 613, 621 (9th Cir. 1979)); *see, e.g.*, *Sosa*, 379 F. Supp. 3d at 222 (in the absence of a prima facie showing of unreasonableness, courts will decline to grant a defendant "an evidentiary hearing so that he may go on a fishing expedition for indicia of unreasonableness"); *Mendlowitz*, 2019 WL 1017533, at *12 & n.13 (denying challenge to reasonableness of search without hearing).

CONCLUSION

For the foregoing reasons, the defendants' motion to suppress should be denied.

Dated: New York, New York
January 31, 2025

Respectfully submitted,

DANIELLE R. SASSOON
United States Attorney

By: /s/
Rushmi Bhaskaran
Nicholas W. Chiuchiolo
Micah F. Fergenson
Georgia V. Kostopoulos
Assistant United States Attorneys
Telephone: (212) 637-2439 / -1247 / -2190 / -2212